Biometric Systems
– Threats and Countermeasures
– The State-of-the-Art

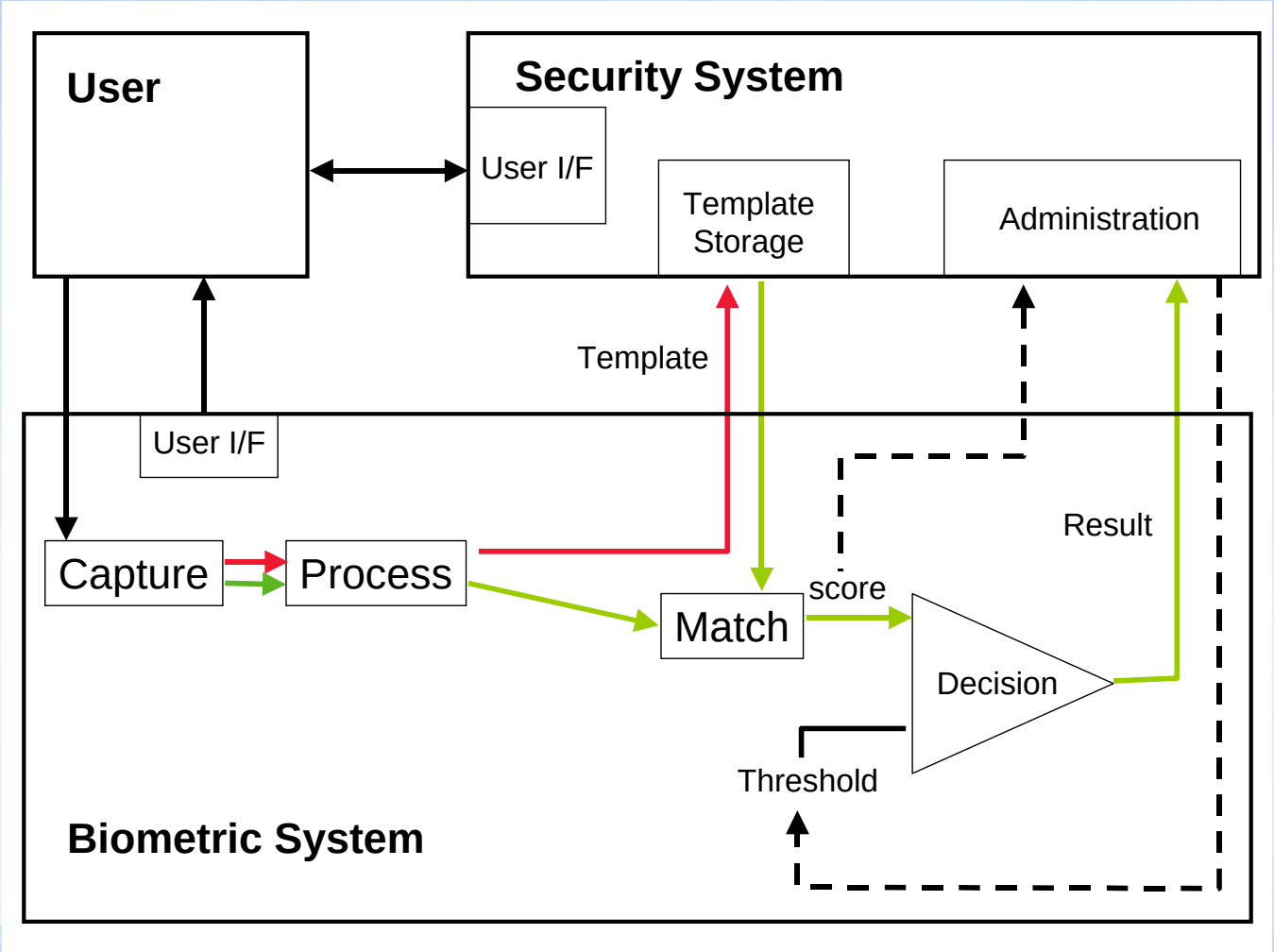
Colin Soutar, CTO, Bioscrypt

Dale Setlak, CTO, Authentec

Overview

- General Biometric System Security
- Security of Biometric Templates
- Security Architecture
- Fake Finger Rejection
- Mutual Authentication

Biometric System and Security System Interface



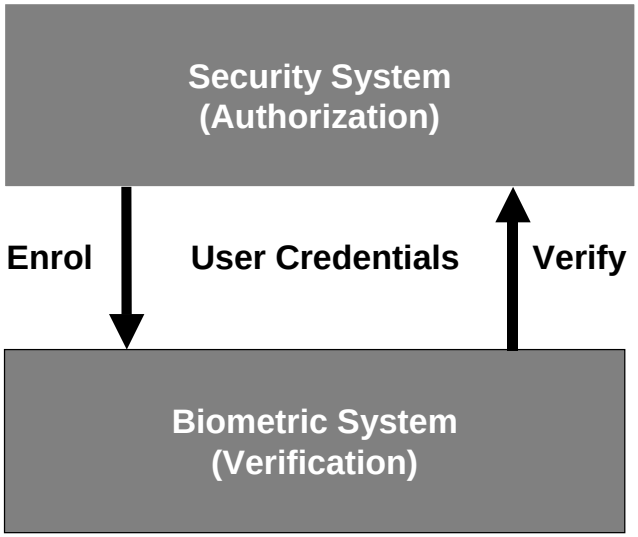
Enrollment/Registration of Individual

- ***registration*** of a new user within security system
- administrator of the system determines the unique ***identity*** of the individual
- new ***user*** established
- a unique ***identifier*** is assigned to the user by which they are known to the security system
- individual instructed to ***enroll*** their biometric to create a biometric ***template***
- template ***bound*** to the identifier, to create a ***user record***

Verification/Authorization of User

- individual establishes a ***claim*** to the system
- user record is ***unbound*** to produce the template and identifier.
- individual is requested to ***verify***
- if a successful match occurs, the identifier is relayed to the security system
- user is ***authorized***, according to their security system rights and privileges

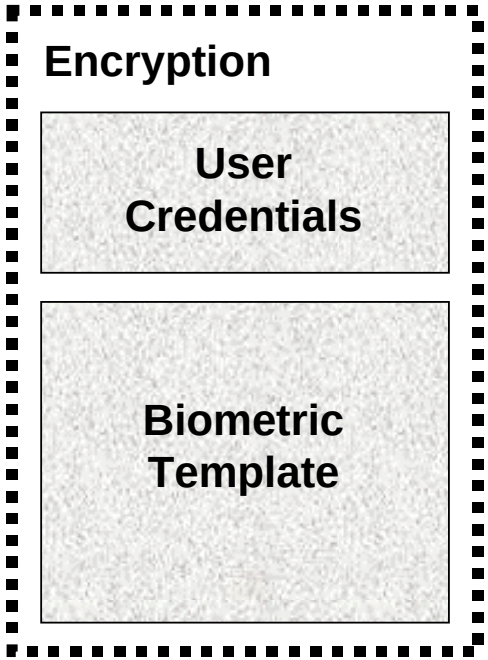
Biometric Verification/User Authorization - User Credentials



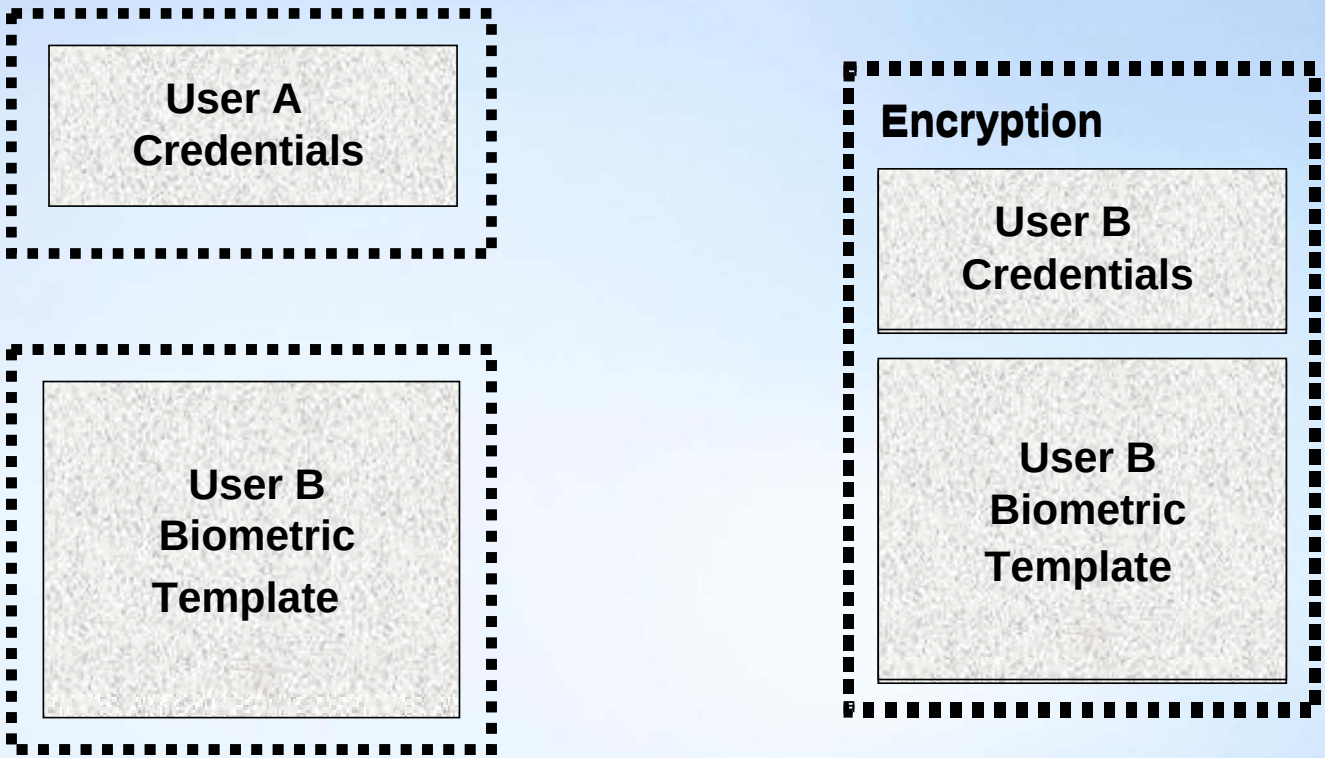
- Link between user verification/system authorization
- Provides complex answer
- Individual can have a number of user credentials
- Prevents Identity Theft

bioscrypt on board

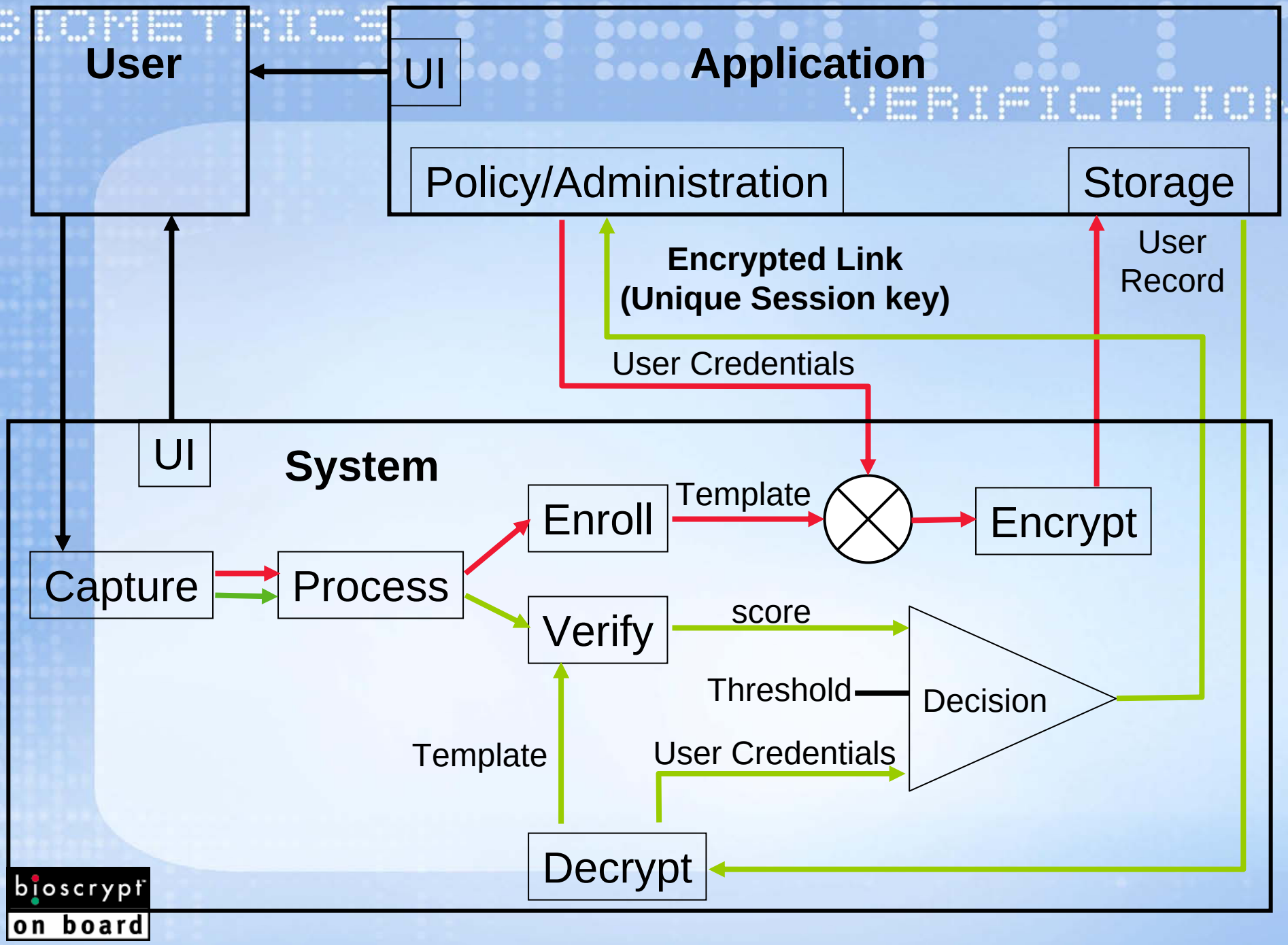
User Record - Encryption



User Record – Encryption
Prevents Identity Theft



bioscrypt on board


User
UI
Application
Policy/Administration
Storage
Encrypted Link
(Unique Session key)
User
Record
User Credentials
UI
System
Enroll
Template
Encrypt
Capture
Process
Verify
score
Threshold
Decision
Template
User Credentials
Decrypt
bioscrypt
on board

System Features

Encryption of User Record

- Provides Confidentiality and Integrity of the biometric template
- Mitigates Identity Theft.

Unique Session Key

- Mitigates replay attack

Use of User Credentials/Identifier

- Mitigates attack on the biometric system result

Internally set threshold

- Avoids threshold-based attacks

Security Evaluation - Common Criteria

- Established in 1998 to provide a mutually recognizable basis for the evaluation of IT security products.
- Designed to replace the existing National Body schemes for security evaluations.

- The Common Criteria comprises three components:
  - Common Evaluation Methodology
  - Protection Profile
  - Security Target

Other System Issues

- Controlled Enrollment/Registration
- User Record/Encryption
- Liveness detection
- Mutual Authentication between components

AuthenTec
The Power of Touch

Overview / Contents

- Context of this discussion
- Interlocked component security architecture
- Real-biometric discrimination – Anti-spoofing
- Mutual authentication between components

)

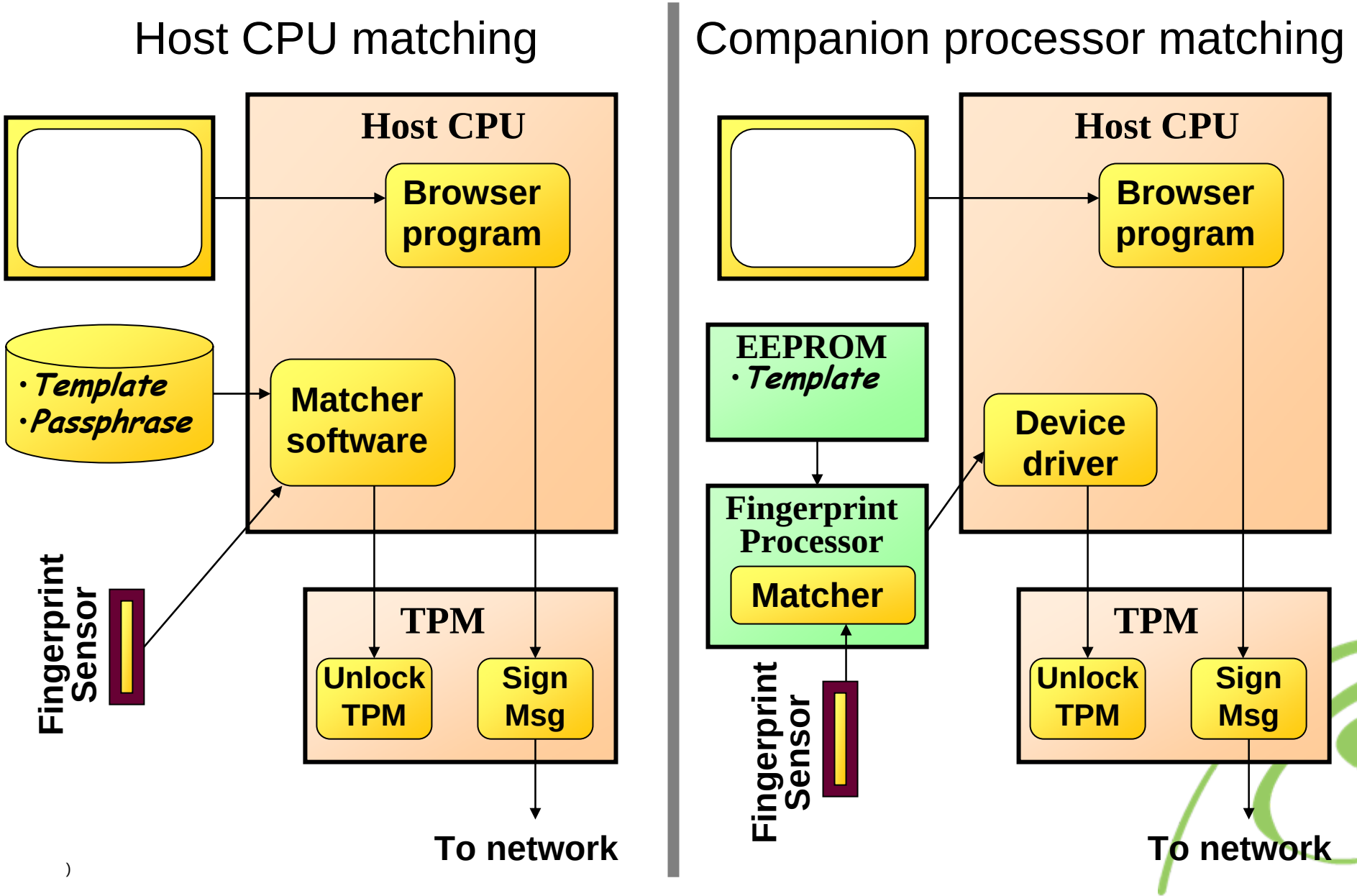
Context for this discussion

- Assumptions
  - Platforms may not be secure
    - Use “Trusted Platform” resources if present
    - Provide best reasonable trust levels when “TP” not present
  - Networks may not be secure
  - Components and their interfaces (SW & HW) can be made reasonably secure
- Approach
  - Balance the security of the ID system with the security of the rest of the system
  - Use interlocked component security chains
    - To provide reasonably secure system-level functions
    - On unsecured platforms and networks

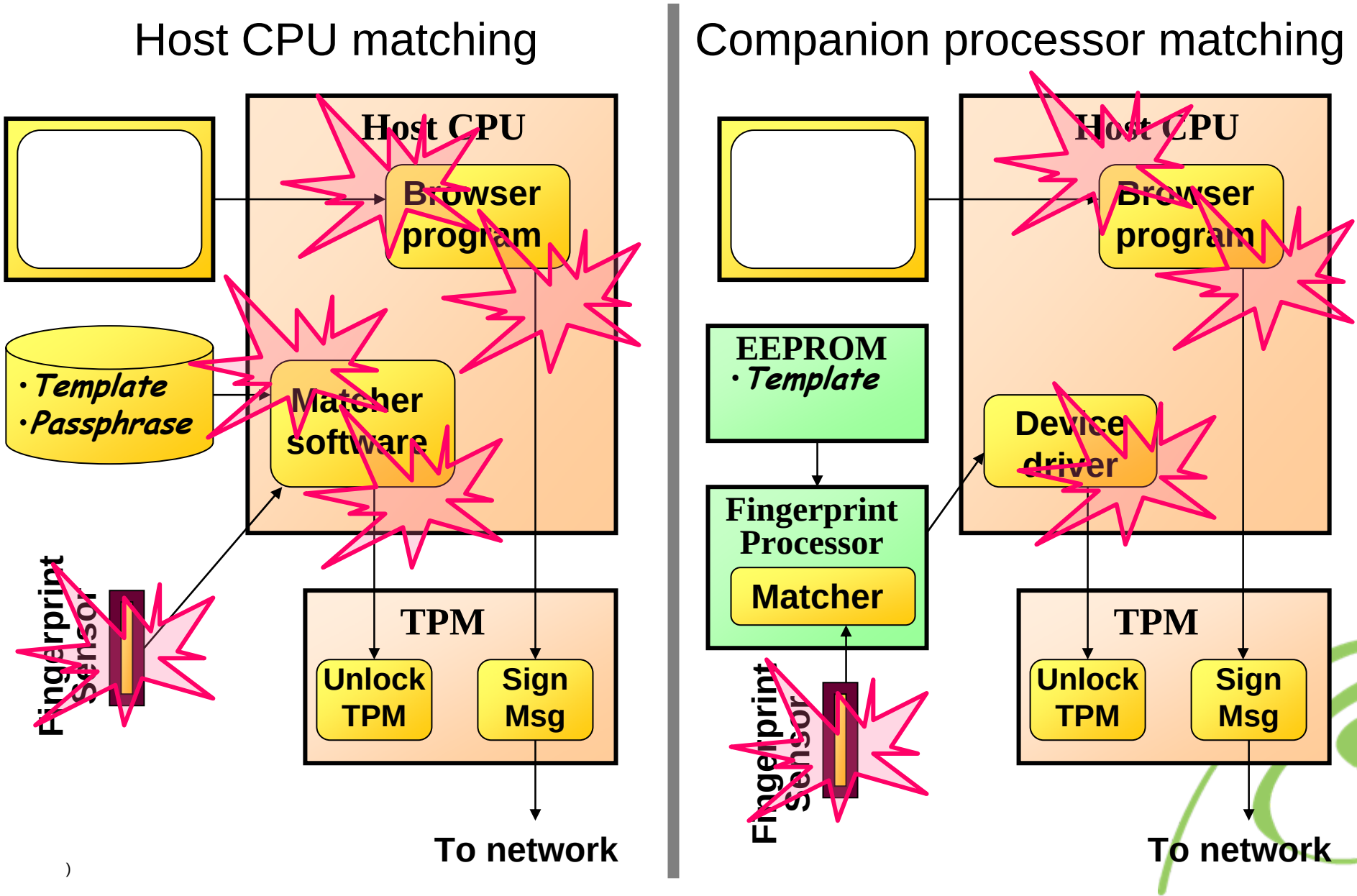
Client Platform

)

A simplified architecture comparison



Some possible attack points



AuthenTec
The Power of Touch

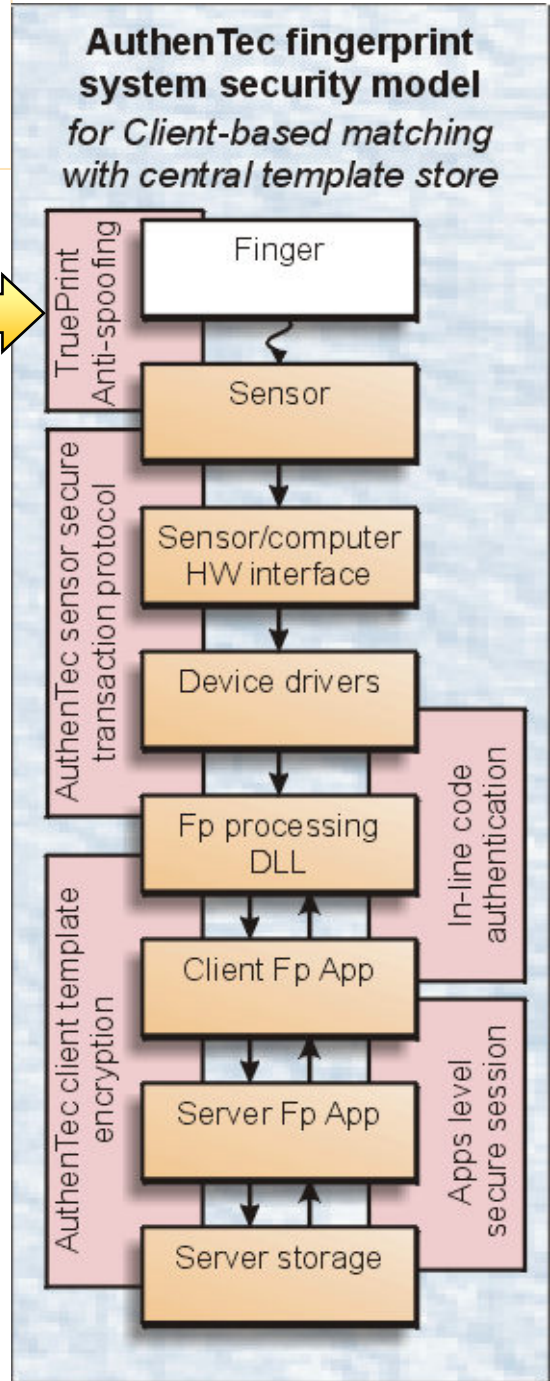
Context for this discussion

- Assumptions
  - Platforms may not be secure
    - Use “Trusted Platform” resources if present
    - Provide best reasonable trust levels when “TP” not present
  - Networks may not be secure
  - Components and their interfaces (SW & HW) can be made reasonably secure
- Approach
  - Balance the security of the ID system with the security of the rest of the system
  - Use interlocked component security chains
    - To provide reasonably secure system-level functions
    - On unsecured platforms and networks

)

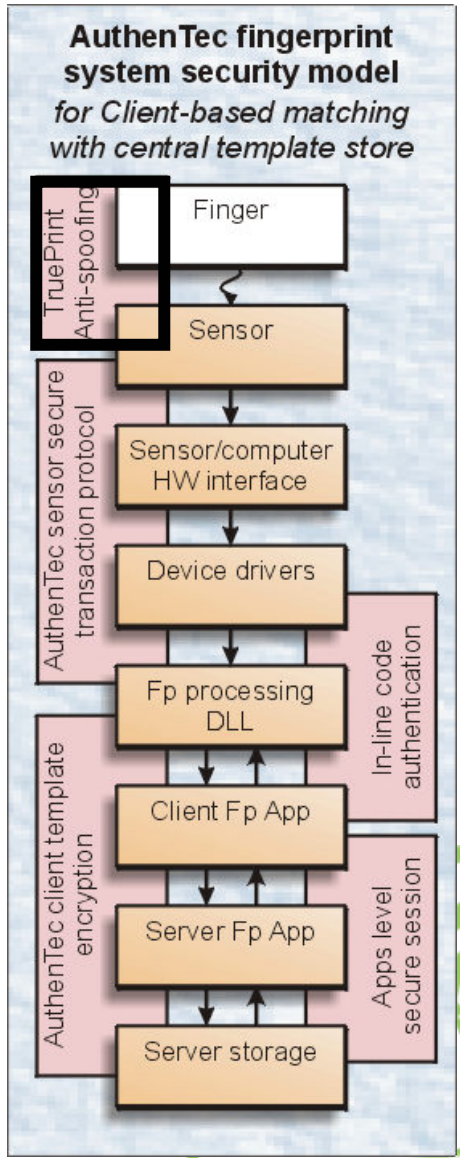
Interlocked component security architecture

- Security starts at the finger-to-sensor interface
  - Spoof detection mechanisms reject fake fingers
- Sensor uses a secure transaction protocol to authenticate each message
  - Uses an on-chip digital signature engine
- Code signing and authentication prevent Software tampering
- Multi-level template encryption and authentication prevent substitutions or insertions
- System level session security links users to privileges



Fake Finger Rejection

- **Definitions:**
  - Fake Finger Rejection = Ability to detect and reject artificial replicas of real fingers
  - Fingerprint pattern data must be treated as publicly available
- **Importance:**
  - Not important in older criminology and background checking applications
    - Use of fake fingers is impractical where sensor use is heavily supervised
  - Critical importance in emerging unsupervised applications
    - E-commerce, E-Banking, general password replacement
    - Personal portable device protection



Biometric Anti-spoofing Approaches

- Class 1. Generic properties of real biometric structures
  - Static properties
  - Dynamic properties
- Class 2. Properties of the real biometric structure that are somewhat specific to the individual
  - Static properties
  - Dynamic properties
- Class 3. Low-selectivity secondary biometric patterns of the structure
  - Static properties
  - Dynamic properties

Skin optical transparency

Cardiac pulse

User specific skin optical transparency

Cardiac pressure profiles

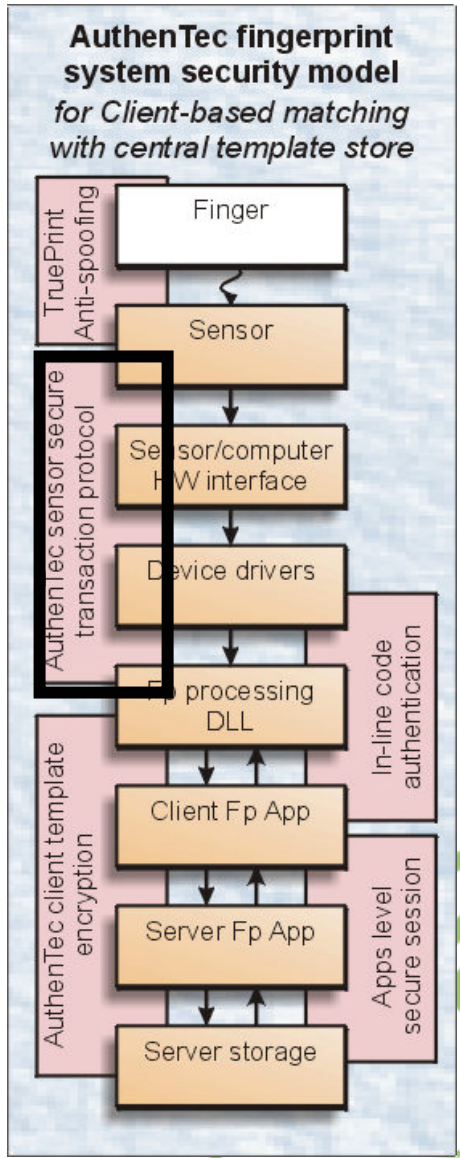
Spectral or spatial pattern of skin optical transparency

Simultaneous Multi-biometric measurements

- Class 3 anti-spoofing
  - Utilize low-selectivity secondary biometric properties
- In fingerprint sensors, Measure multiple biometric properties of the finger
  - Fingerprint PLUS other properties
  - **Characteristics of the best biometric properties:**
    - Unrelated to friction ridge pattern (biometrically orthogonal)
    - Cannot be deduced from info in a latent fingerprint
    - Somewhat different from one person to the next
    - Reasonably uniform distribution across the population
    - Somewhat stable for a single finger over time
- Characteristics of the measurements
  - Measurements made simultaneously
  - Measure the same physical structure
  - Use colocated sensing devices

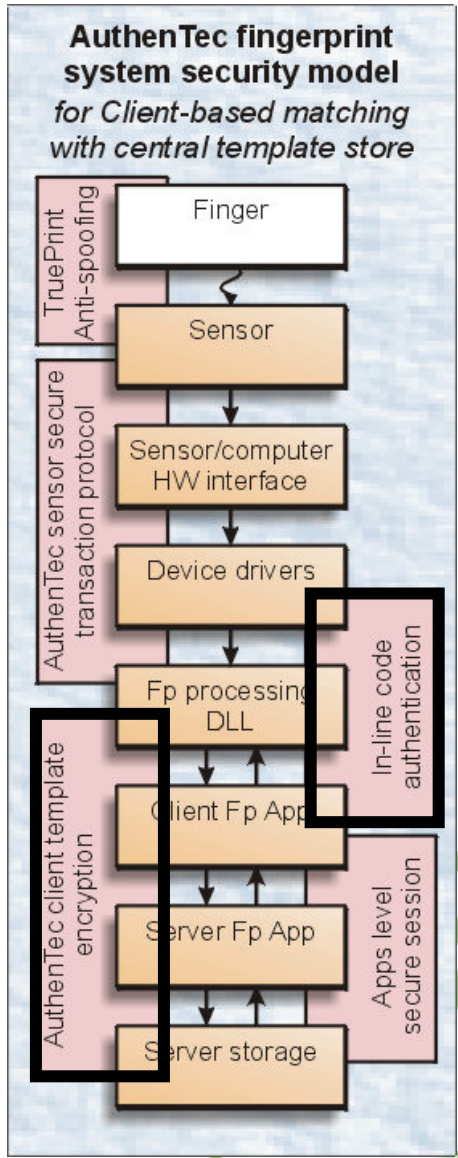
Sensor Secure Transaction Protocol

- Protects against
  - Threats to the “wire” between the sensor and the host computer
  - Attacks on the I/O drivers or device drivers
  - Including: record/replay, man-in-the-middle, device substitution, etc
- Protocol overview
  - The processor sends a new challenge word to the sensor before each image is captured
  - The challenge word is used with codes internal to the sensor to produce an encryption key
  - Each image is digitally signed using the image data and this encryption key
  - Each image’s signature is verified when that image is processed



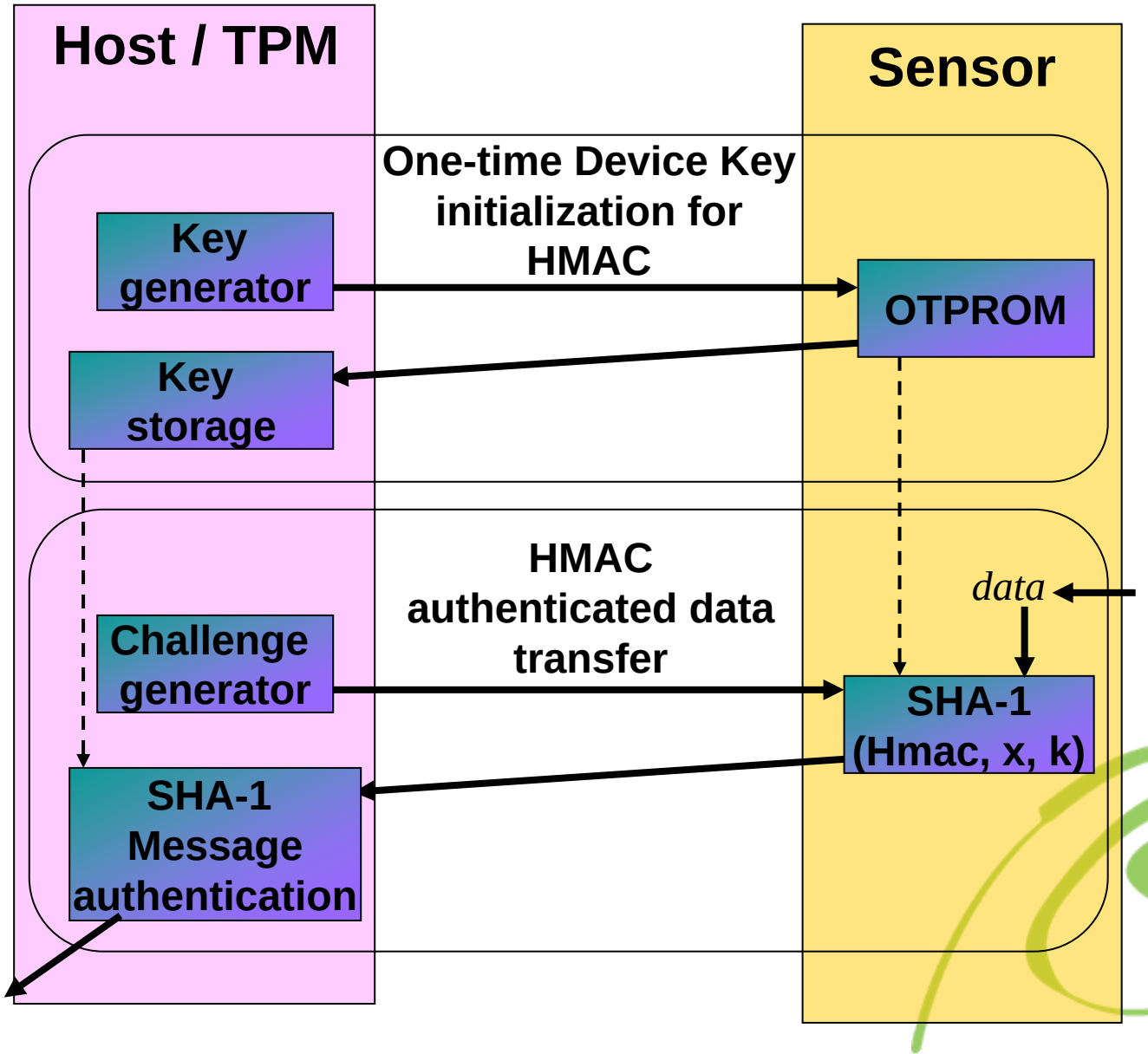
Securing the software services

- Objective
  - Make the software and data as secure as practical
    - Within the limits of current commercial platforms
  - Architecture must provide clean transition path
    - Provide reasonable security on existing platforms
    - Support TPM services where available
    - Support trusted platform
      - when infrastructure support becomes available



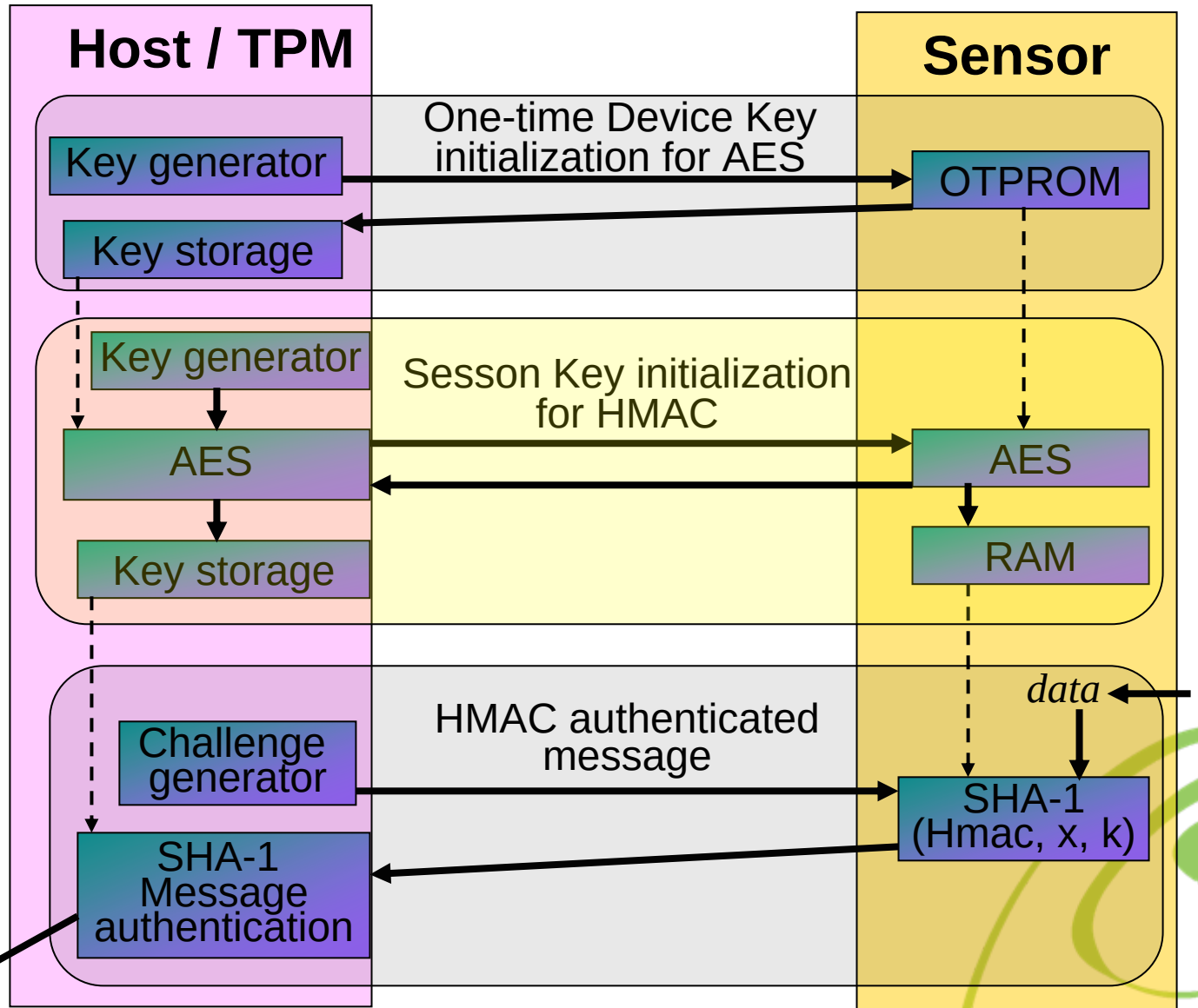
Example minimum stationary input device transactions

- Sensor key init
  - performed in secure environment
  - Either during:
    - Mfg. init.
    - Sys Mgr config
    - Initial user enroll
- Trusted device is
  - Combo of periph. device + TPM
  - For remote usage, TPM rehashes and then signs data
    - Allows device key to remain local
  - Key mgmt with the remote server via TPM PKI



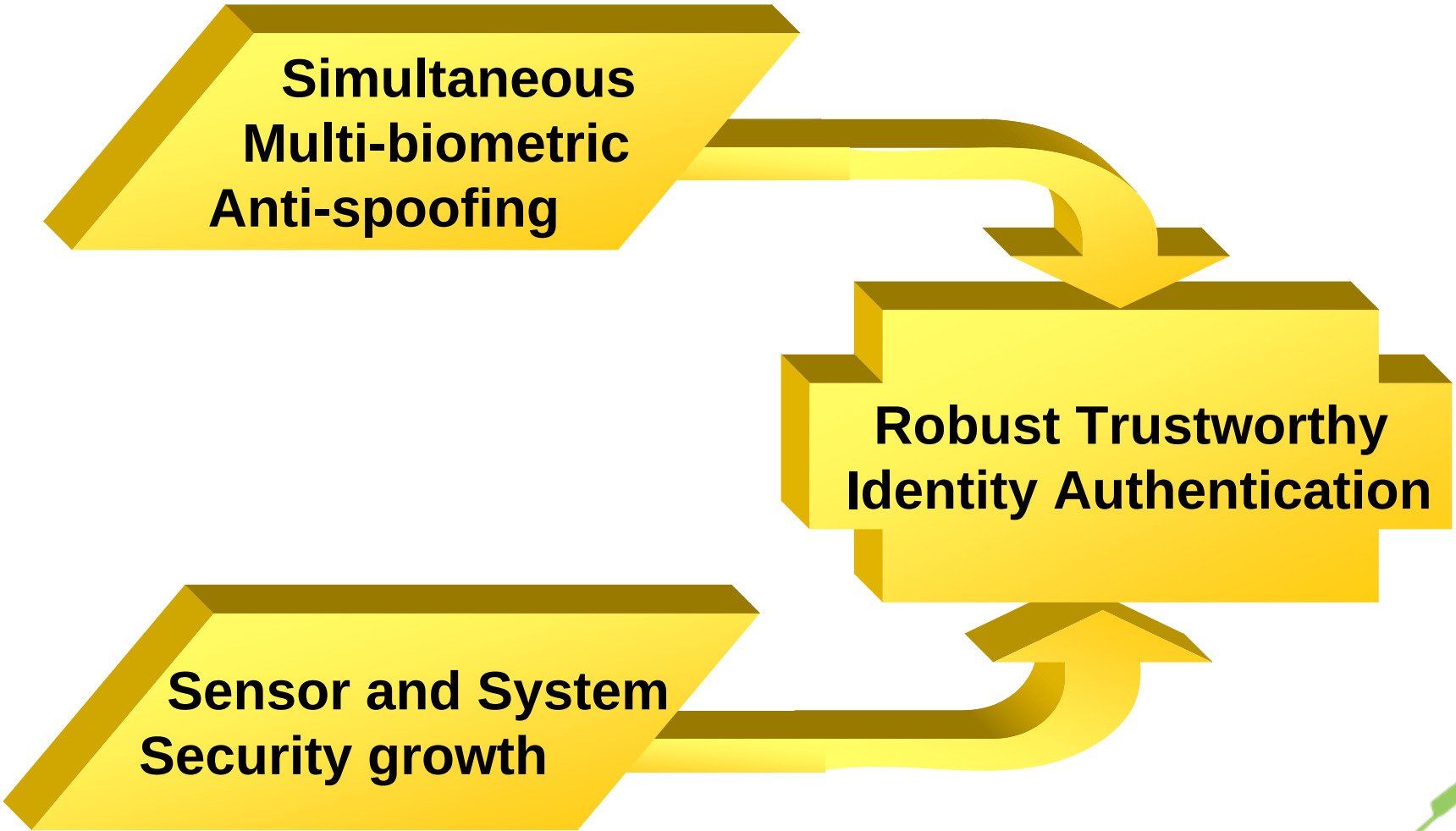
Session keys for stationary input device

- Session key initialization
  - Add a third transaction type for session key init
  - performed every time device is powered up
- Trusted device is
  - Combo of peripheral device + TPM
  - Session keys can be generated remotely and used for verification remotely (e.g. MS server)
  - No rehashing by the TPM is required
  - Key mgmt with server via TPM PKI



AuthenTec
The Power of Touch

Putting It All Together



)